COMMUNICATIONS ALLIANCE LTD

Inquiry into Privacy Amendment (Privacy Alerts) Bill 2013 - Submission to Senate Standing Committee on Legal and Constitutional Affairs

COMMUNICATIONS ALLIANCE SUBMISSION

JUNE 2013

Introduction

Communications Alliance welcomes the opportunity to provide comment on the Privacy Amendment (Privacy Alerts) Bill 2013 (the Bill). Communications Alliance emphasises at the outset that the telecommunications industry takes the privacy of customers very seriously. In our view, it is good business practice to take every precaution to protect a customer's privacy and this is a fundamentally matter of principle for the industry. For any business to have a productive ongoing relationship with a customer, it needs to develop – and maintain – a level of trust, including in relation to privacy.

Communications Alliance provided a submission to the Attorney-General's Department on the Exposure Draft of the Bill. In that submission, Communications Alliance raised a number of concerns relating to the Bill, including unreasonable timeframes for comment and lack of consultation with industry, as well as specific issues relating to the contents of the Bill. In summary these concerns included that:

- industry has not been given sufficient time to consider the contents of the Bill and the cost implications of the introduction of mandatory measures;
- there is already a voluntary guide which provides industry with appropriate guidance relating to serious privacy breaches;
- the Bill contains a number of deficiencies such as:
    - the lack of a definition of 'serious harm';
    - the fact that it gives greater priority to immediate notification of customers than to limiting the potential breach;
    - the discretion of the Commissioner to direct an entity to notify, with no right of appeal being afforded ;
- industry is already required to resource implementation of the measures contained in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012,* which commences in March 2014 and objects to any additional burden at this time.

It would seem that the legitimate concerns of industry have been paid little regard , in favour of rushing through impractical legislation which will result in costly, and unnecessary, burdens on industry.

About Communications Alliance

Communications Alliance is the primary telecommunications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to provide a unified voice for the telecommunications industry and to lead it into the next generation of converging networks, technologies and services. The prime mission of Communications Alliance is to promote the growth of the Australian communications industry and the protection of consumer interests by fostering the highest standards of business ethics and behaviour through industry self-governance. For more details about Communications Alliance, see http://www.commsalliance.com.au.

Section 1: Timing of the Bill and Inadequate Consultation

The Government previously committed – and industry and other stakeholders agreed - to a staged process of consultation on privacy law reform. Consideration of the issue of a mandatory privacy breach notification scheme was to be postponed until a second stage of review of Australian privacy law following the Australian Law Reform Commission (ALRC) Report 108.

The telecommunications industry is already investing significant resources to implement the measures in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Enhancing Privacy Protection Act) which come into effect in March 2014. It is regrettable that concerns regarding the tight timeframe to review the Bill, lack of consultation with industry and requests for a delay to implement proposed measures appear to have been dismissed by Government.

Communications Alliance re-emphasises that it would be to the benefit of all – that is, the business community and consumers - that this legislation is delayed. Industry should be given adequate opportunity to consider, and have input to, the proposed introduction of a mandatory data breach notification scheme as proposed by the original consultation schedule.

Section 2: Contents of the Bill

Definition of 'Serious Harm'

Communications Alliance has genuine concerns about the lack of definition of 'serious harm'.
26X(2)(d)(i) of the Bill states that '*…the access or disclosure will result in a real risk of serious harm to any of the individuals…*'.

In industry's view, there should be a threshold test that industry can use to determine whether 'serious harm' could or would be caused. It is noted that both 'risk' and 'real risk' are defined within the legislation, as well as 'harm' but there has been no attempt to define the concept of 'serious harm'.

Further, in the absence of a definition of 'serious harm', it is possible that the legislation will cause an organisation to take a risk-averse position in order to avoid breaching such an obligation. This could, potentially, result in over-reporting of relatively minor data-related errors.

Obligation to Prioritise Notification

The current voluntary Data Breach Notification Guide (Guide) of the Office of the Australian Information Commissioner (OAIC) provides guidance to industry on matters relating to a breach of privacy. While it is difficult to quantify compliance with the Guide, there is anecdotal evidence to suggest that there is a high level of compliance within the telecommunications industry.

The Guide sets out the following steps to consider when responding to a data breach or suspected breach:

- Contain the breach and do a preliminary assessment;
- Evaluate the risks associated with the breach;
- Notification; and
- Prevent future breaches.

The Guide provides a degree of flexibility and allows businesses to consider each breach on a case-by-case basis. This is in contrast to the requirements in the Bill, as set out below.

26ZB sets out the order of processes that an entity must undertake immediately after a serious data breach has occurred. In our view, the order of actions that must be undertaken is contrary to the way in which good business practice would dictate, already outlined in the voluntary Guide. That is, good business practice would be to (a) contain the breach and do an assessment; (b) evaluate the risks; and then, if necessary, notify those affected by the breach. It is concerning that the Bill places more emphasis on notifying – and potentially confusing or alarming customers – than containing the breach, rectifying the issue and preventing its reoccurrence.

Once again, the current Guide provides much more flexibility in this regard and allows entities to determine on a case-by-case basis what actions should be taken. It is our view that the intent of processes to manage serious breaches of privacy should be on making good the harm that has been done, rather than causing unnecessary alarm.

No Right to Appeal a Commissioner's Direction

26ZC(1) of the Bill states that if the Commissioner has 'reasonable grounds' to believe there has been a serious breach then he/she may direct an entity to undertake a process to notify. In addition, 26ZC(4) states that 'an entity must comply with a direction… as soon as practicable after the direction is given'.

Communications Alliance has serious concerns that these clauses provide no opportunity for an organisation to appeal such a determination. It is only reasonable that an entity should have an opportunity to have a right of reply, particularly in circumstances in which the Commissioner may be acting according to misinformation.

Section 3: Significant Cost to Implement Obligations in the Bill

Communications Alliance would question the veracity of the Regulation Impact Statement (RIS) and its assessment of the costs and benefits of the proposed Bill. As stated above, the telecommunications industry is already investing significant resources implementing other privacy reforms by March 2014. Given the haste with which this Bill was prepared and introduced to Parliament, it is unreasonable to assume that because there was not agreement on the cost of implementation of a mandatory data breach notification scheme, that these costs would not be significant or that this concern should be dismissed. The RIS states:

> *"The targeted consultation process did not receive specific costs estimates. There was no common view among respondents about the likely amount of costs, with respondents providing a broad range of general cost estimates on this issue….On the other hand, privacy and consumer advocates argued that the costs would be minimal.*
>
> *However, specific costs estimates varied from a small group of stakeholders who believed there would be large costs amounts to most who believed there would be modest cost implications. Privacy and consumer advocates believed costs would be minimal, and should be considered necessary where an entity handled personal information."*

Given the limited consultation undertaken, it would be fair to say that industry was given very limited opportunity to consider the contents of the Bill, let alone determine the costs associated with its implementation. Further, it would seem unlikely that consumer advocates are best placed to make any estimate of the costs of implementing the reforms on business.

As Communications Alliance stated in its submission to the Attorney General's Department, the implementation of a mandatory data breach system is likely to be costly. This, of course, may depend on what current systems are in place within each business, as well as the costs of ensuring compliance with a mandatory scheme.

Additionally, it would seem likely that there would be some correlation of cost with the amount of data held by an entity and also whether it is held locally or offshore. It is also difficult to attempt to quantify the cost of communicating a breach to those affected until the breach has occurred. That is, until an entity has an understanding of the size and nature of a breach, how can it determine the cost of notification?

However, what is indisputable is that moving from a voluntary Guide to mandatory legislation will result additional costs to business, including legal counsel, associated with ensuring compliance with a mandatory scheme. That is, what could once be managed through good internal business processes would need be formalised in such a way as to require businesses to seek expert advice to ensure they comply with legislative requirements.

As previously submitted, given all of these unknowns, additional time is needed to consider these issues in a detailed consultation process, rather than rushing through amendments based on industry's 'best guess'.

Section 4: Timeframe for Implementation of Mandatory Privacy Breach Notification Scheme

Communications Alliance is strongly opposed to the introduction of any additional regulatory obligation relating to the introduction of a mandatory privacy breach notification scheme. However, if the Bill were to pass, the period between passage of the legislation and implementation should be a minimum of 15 months as was the case with the Enhancing Privacy Protection Act.

Section 5: Workload of the Office of the Australian Privacy Commissioner

Communications Alliance is cognisant of concerns raised in relation to the current resourcing and workload of the OAIC. Given the demands involved in implementing the measures in the Enhancing Privacy Protection Act, there are legitimate concerns as to the ability of the OAIC to cope with any additional workload.

Communications Alliance therefore believes it is an inappropriate time to introduce a mandatory privacy breach notification scheme which will further burden the OAIC. Any diversion of resources away from implementing the measures included in the Enhancing Privacy Protection Act, to the introduction of a mandatory privacy breach notification scheme, may put at risk the timely introduction of important privacy reforms.

Section 6: Privacy Breaches – Fraudulent and Intentional

While it is important not to diminish the unfortunate circumstances when a privacy breach occurs as a result of an error by a business, it should be acknowledged that an infringement of privacy is much more likely to be attributable to cyber criminals or other rogue operators than legitimate businesses. In these circumstances, the breach of privacy is intentional and done with the aim of using personal information to cause damage or harm.

A requirement for business to establish mandatory privacy breach notification processes without other appropriate complementary cyber-security legislation, places a disproportionate burden on business while doing nothing to address the majority of fraudulent activity that causes intentional harm.

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 9
32 Walker Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507